

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-240945

(43)Date of publication of application : 26.08.2004

(51)Int.Cl.

G06F 13/00

(21)Application number : 2003-159848

(71)Applicant : DEEPSOFT CO

(22)Date of filing : 04.06.2003

(72)Inventor : HA JEONG HO

AHN JAE GEUN

KAN SUHON

(30)Priority

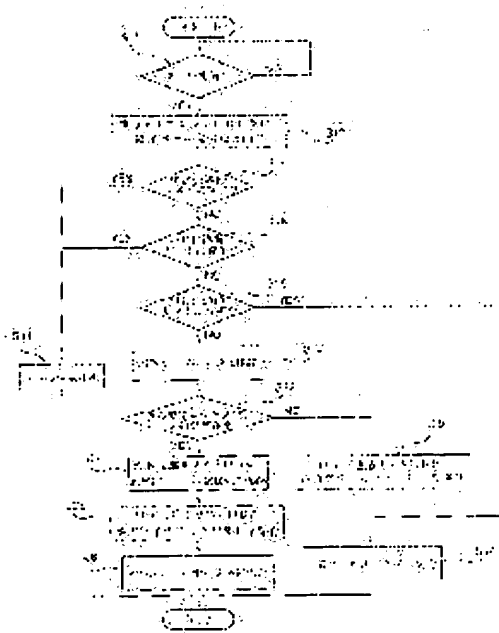
Priority number : 2003 200307982 Priority date : 08.02.2003 Priority country : KR

(54) AUTOMATIC SHUTOFF METHOD OF SPAM MAIL THROUGH DYNAMIC URL CONNECTION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an automatic shutoff method of spam mail through dynamic URL connection capable of straining a spam mail and automatically shutting off it.

SOLUTION: This automatic shutoff method of spam mail through dynamic URL connection is performed in an e-mail system where a number of mail servers are connected through the Internet. This method comprises steps of extracting dynamic URL information present in the message original of an e-mail received; performing the connection to a Web page linked with the extracted dynamic URL information; and classifying the received e-mail as a spam mail when a preliminarily regulated spam keyword is present in the content of the Web page.



【特許請求の範囲】**【請求項1】**

多数のメールサーバがインターネットを通じて連結されてなる電子メールシステムで行われるスパムメール自動遮断方法において、
受信される電子メールのメッセージ原本に存するダイナミックURL情報を抽出する段階
；
前記抽出されたダイナミックURL情報にリンクされたウェブページに接続を行なう段階
；及び
前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存する場合に前記受信電子メールをスパムメールとして分類する段階を含んでなることを特徴とするダイナミックURL接続を通じたスパムメール自動遮断方法。

【請求項2】

前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存する場合に前記受信電子メールの発信元を前記メッセージの原本から抽出して発信元遮断リストデータベースに保存し、今後前記発信元遮断リストデータベースに存する発信元からの電子メールの受信を拒否することを特徴とする請求項1に記載のダイナミックURL接続を通じたスパムメール自動遮断方法。

【請求項3】

前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存する場合に前記ダイナミックURL情報をURL遮断リストデータベースに保存し、今後前記URL遮断リストデータベースに存するダイナミックURL情報がメッセージ原本に含まれた電子メールの受信を拒否することを特徴とする請求項1に記載のダイナミックURL接続を通じたスパムメール自動遮断方法。

【請求項4】

前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存する場合に前記受信電子メールの発信元を前記メッセージ原本から抽出して発信元遮断リストデータベースに保存し、今後前記発信元遮断リストデータベースに存する発信元からの電子メールの受信を拒否することを特徴とする請求項3に記載のダイナミックURL接続を通じたスパムメール自動遮断方法。

【請求項5】

前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存しない場合に一般メールとして分類し、前記ダイナミックURL情報を前記メッセージ原本から抽出してURL通過リストデータベースに保存し、今後前記URL通過リストデータベースに存するダイナミックURL情報がメッセージ原本に含まれた電子メールを一般メールとして分類することを特徴とする請求項1ないし4のうちのいずれか1つに記載のダイナミックURL接続を通じたスパムメール自動遮断方法。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明はダイナミックURL接続を通じたスパムメール自動遮断方法に関するものであって、特に受信された電子メールにリンクされているURL情報を抽出して該当ウェブページに接続した後、予め規定された所定のスパムキーワードがある場合これをスパムメールとして濾し出して自動で遮断することができるようにしたダイナミックURL接続を通じたスパムメール自動遮断方法に関するものである。

【0002】**【従来の技術】**

よく知られたとおり、電子メールシステムというのはインターネットを通じて特定なユーザとデータやメッセージを交換するシステムを言い、スパムメール(Spam-Mail)というのは受け取る方の意向を無視し大量にまき散らす広告、宣伝、勧誘などの商業的な目的を有する電子メールを言う。さらに広範囲的には、明示的な受信拒否意思に反する

営利目的の広告性情報メール、システム性能を低下させる目的で発送する大量メール、プログラム著作権を侵害する不法ソフトウェアなどの販売広告メール、公序良俗を害する成人用品及び不健全サイトなどの広告メール及び恐怖心や不安感を引き起こすメールなどがスパムメールと見做され得る。

【0003】

一方、このようなスパムメールが受信者に与える弊害を最小化するために韓国政府では情報通信網利用促進及び情報保護などに関する法律及びその下位法において多様かつ具体的なスパムメールの制限規定を備えておいてこれに違反する場合には所定の罰を課することができるよう措置している。一例に、スパムメールの題名の頭に“(広告)”や“(成人広告)”というキーワードを必ず表示するように規定しているが、受信者がスパムメール汚過プログラムを設置した後にこのようなキーワードを題名として有する電子メールをスパムメールとして分類するように設定すれば今後このような題名を有する電子メールが自動的にスパムメールとして分類されるようになる。さらに現在はメールクライアントがスパムメール汚過のための任意キーワードを設定することもでき、題名または本文の内容中に前記設定キーワードを含んでいる電子メールが自動でスパムメールとして分類されるようになっている。以下、このような従来のスパムメール遮断方式を‘自体定規表現式’という。

【0004】

一方、スパムメールとして渡し出されるのを避けるための努力も一層強化されているが、特に成人用サイトの広告メールの場合には平凡なメールの題名下に本文にはイメージのみを含ませた状態で成人用サイトのホームページURL(Uniform Resource Locator)をリンクする方式が多く使用されている。

【0005】

【発明が解決しようとする課題】

しかし、前述した従来の技術によると、受信電子メールの題名または本文の中にメールクライアントが設定したスパムキーワードが存するかどうかを検査するだけで、本文の内容にリンクされたURLに接続されるウェブページのコンテンツまでは検査しないため、前記のような変形されたスパムメールを全く渡し出すことができないという問題点がある。

【0006】

本発明は前述した問題点を解決するために案出されたものであって、本発明の目的は、受信された電子メールにリンクされているURL情報を抽出して該当ウェブページに接続した後、予め規定された所定のスパムキーワードがある場合、これをスパムメールとして渡し出して自動で遮断することができるようにしたダイナミックURL接続を通じたスパムメール自動遮断方法を提供するところにある。

【0007】

【課題を解決するための手段】

前述した目的を達成するために本発明のダイナミックURL接続を通じたスパムメール自動遮断方法は、多数のメールサーバがインターネットを通じて連結されてなる電子メールシステムで行われるスパムメール自動遮断方法において、受信される電子メールのメッセージ原本に存するダイナミックURL情報を抽出する段階；前記抽出されたダイナミックURL情報にリンクされたウェブページに接続を行なう段階；及び前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存する場合に前記受信電子メールをスパムメールとして分類する段階を含んでなることを特徴とする。

【0008】

前述した構成において、前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存する場合に前記受信電子メールの発信元を前記メッセージ原本から抽出して発信元遮断リストデータベースに保存し、今後前記発信元遮断リストデータベースに存する発信元からの電子メールの受信を拒否するのが好ましい。

【0009】

好ましくは、前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存

する場合に前記ダイナミックURL情報をURL遮断リストデータベースに保存し、今後前記URL遮断リストデータベースに存するダイナミックURL情報がメッセージ原本に含まれた電子メールの受信を拒否する。

【0010】

好ましくは、前記ウェブページのコンテンツのうち予め規定されたスパムキーワードが存しない場合に一般メールとして分類し、前記ダイナミックURL情報を前記メッセージ原本から抽出してURL通過リストデータベースに保存し、今後前記URL通過リストデータベースに存するダイナミックURL情報がメッセージ原本に含まれた電子メールを一般メールとして分類する。

【0011】

【発明の実施の形態】

以下、本発明の好ましい実施形態を添付の図面を参照して詳しく説明する。本実施形態は本発明の権利範囲を限定するのではなく、ただ例示として提示したものである。

【0012】

図1は一般的な電子メールシステムのネットワーク構成図であって、一般的な電子メールの送/受信はインターネット30に連結された電子メールクライアント(以下、'メールクライアント'という)18が自体ウェブサイト10に備えられたメールサーバ(以下、'自体メールサーバ'という)12または自体ウェブサイト外部から電子メールサービスを提供する各種ウェブサイト、例えば大小のポータルサイトやISP(Internet Service Provider)のウェブサイト20に備えられたメールサーバ(以下、'外部メールサーバ'という)24から電子メールアカウントを付与され行なうことができる。

【0013】

自体ウェブサイト10はウェブ文書処理するウェブサーバ14とメールの送/受信を担当するメールサーバ12及びメールクライアント18が構内網16、例えばLANやイントラネットを通じて連結されてなされる。勿論、夫々の外部ウェブサイト20にもウェブサーバ22とメールサーバ24が備えられている。図面において未説明符号40は自体のウェブサイトを備えていないまま、主に家庭や個人事務室などで電話回線やケーブル、衛星、ADSL、ISDNなどを通じてインターネット30に接続する個人メールクライアントであるところ、このような個人メールクライアント40は主に外部メールサーバ24に加入してメールアカウントを無料で割り当てられた後で、電子メールサービスを利用する。勿論、自体ウェブサイト10に属したメールクライアント18も外部メールサーバ24に加入して電子メールサービスを利用することができる。

【0014】

一方、前述した電子メールシステムにおいて、任意の発信側メールクライアントが内部メールサーバ12または外部メールサーバ24を通じて送った電子メールはSMTP(Simple Mail Transfer Protocol; 簡易メール伝送プロトコル)により受信側のメールクライアントの電子メールアドレスとして代表される内部または外部メールサーバ12、24のメールボックスに伝送された後に保管される。以降、受信側メールクライアントはインターネット30を通じて自分のメールボックスに接続してそこに保存されている電子メールを読み取ることができる。受信側のメールクライアントが自己受信の電子メールを読み込んで来る方式ではメールサーバ12、24のメールボックスに保存されている電子メールをメールクライアントコンピュータのハードディスクにコピーする方式であるPOP3(Post Office Protocol#3:メールサーバから電子メールを受け取って来るための郵便局プロトコル)方式及び自己受信の電子メールをメールクライアントコンピュータにコピーする必要なしにメールボックスに保存させた状態で利用することができるようにするIMAP(Internet Message Access Protocol)方式などがあるところ、このようなPOP3やIMAPは通常的に内部メールサーバシステムで多く採用している。

【0015】

一方、最近にはIMAPに加え、インターネットに受信メールを保存しておいて、どこからでもアクセスすることができるようにするウェブメールサービスが登場したが、このようなウェブメールを簡単に説明するとメールサーバとウェブサーバが合体したサービスと言える。即ち、メールクライアント側から見たウェブメールサーバは一般ウェブサーバと全く同じ形態を有しているところ、従ってメールクライアントがウェブメールサーバにアクセスするためにはウェブブラウザだけあれば良く、電子メールソフトウェアは必要がない。このようなウェブメール機能は各種ポータルサイトやISPなどでサービス次元で無償で提供している。

【0016】

図2は本発明の一実施形態によるURL情報抽出を通じたスパムメール自動遮断方法を説明するためのフローチャートであるところ、本発明のスパムメール自動遮断方法によるプログラム（以下、‘スパム遮断プログラム’という）は内部または外部メールサーバ12、24に統合されたり別個で設置され得るし、且つ個人メールクライアント40の場合にはクライアントコンピュータの電子メールソフトウェアに統合されたり別個で設置されることができる。

【0017】

また、以下で‘スパムキーワード(Keyword)’というのはスパムメールにおいてよく使用される2つ以上の文字の集合を言う。例えば、前記スパムキーワードは公序良俗に反する成人用品及び不健全サイトなどの広告メールに頻繁に使用される‘セックス(sex)’、‘オーガズム’、‘ヌード’、‘ホルノ’‘ヤドン(いやらしい動映像の略語)’、‘変態’、または‘自慰’などが含まれ得る。

【0018】

図2に示したとおり、先ず段階S10において任意の電子メールが受信された場合にスパム遮断プログラムは段階S12を行なって受信された電子メールのメッセージ原本にリンクされているウェブページ（以下、‘ダイナミックURL’という）及び電子メールの発信元Eメールアドレス（以下、‘電子メール発信元’という）を抽出する。

【0019】

例えば、図3は本発明の一実施形態による受信された電子メールのポップアップウィンドウを示した図であり、図4は本発明の一実施形態による受信された電子メールのメッセージ原本を示した図である。

【0020】

図3及び図4に示したとおり、通常の電子メールはヘッダー(header)部とボディ部(Body)に分けられるが、前記ヘッダー部には電子メールを正しく配送するために必要な電子メール発信元(sda35s5g32-13@yahoo.com)及びメッセージの題名などが記載されており、前記ボディ部には例えば、本文の内容(ナイスパディーなくせに……)と広告しようとする成人用サイトのホームページのURL(href="http://www.ohmybuin.com/index.asp?ID=3956623")及びリンクされている複数のイメージ100情報が含まれているイメージURL(IMG alt=OhMyBuin.Com height=85src="http://www.ohmybuin.com/banners/title.gif" width=504)情報のみが記載されている。

【0021】

次に、段階S14に進んで、前記電子メール発信元が発信元遮断リスト(データベース)に登録されたアドレスであるかどうかを照会することになるが、このためのスパム遮断プログラムは発信元遮断リストDB(データベース)を運用しなければならない。

【0022】

段階S14における判断の結果、前記電子メールの発信元が発信元遮断リストに登録されている場合には段階S34に進み、当該電子メールの受信を拒否、例えば本文の内容を読まないまますぐ削除処理をすることになる。これによってメールサーバ(またはクライアント)が当該電子メールがスパムメールであるかどうかを確認するのに伴う負荷を軽減さ

せることができる。

【0023】

一方、段階S14における判断の結果、前記電子メールの発信元が発信元遮断リストに登録されていない場合には段階S16に進み、前記ダイナミックURLがURL遮断リスト（データベース）に登録されたウェブページの住所であるかどうかを照会することになるが、このためのスパム遮断プログラムはURL遮断リストDB（データベース）を運用しなければならない。

【0024】

段階S16における判断の結果、前記ダイナミックURLがURL遮断リストに登録されている場合には段階S34に進み、当該電子メールの受信を拒否することになる。

【0025】

一方、段階S16における判断の結果、前記ダイナミックURLがURL遮断リストに登録されていない場合には段階S18に進み、前記ダイナミックURLがURL通過リスト（データベース）に登録されたウェブページのアドレスであるかどうかを照会することになるが、このためにスパム遮断プログラムはURL通過リストDB（データベース）を運用しなければならない。

【0026】

段階S18における判断の結果、前記ダイナミックURLがURL通過リストに登録されている場合には段階S32に進み、当該電子メールを一般メールボックスに保存する。

【0027】

反面、段階S18における判断の結果、前記ダイナミックURLがURL通過リストに登録されていない場合には段階S20に進み、前記ダイナミックURLを利用して当該ウェブページに接続を行なうことになる。

【0028】

次に、段階S22に進み、接続されたウェブページのコンテンツ（Contents）を検索して自体的に運用するスパムキーワードデータベースに予め規定された通りのスパムキーワードが存するかどうかを判断する。段階S22における判断の結果、当該接続されたウェブページのコンテンツに規定されたスパムキーワードが使用されていない場合には前記URL通過リストDB（データベース）に該当電子メールのダイナミックURLを保存する。

【0029】

一方、段階S22における判断の結果、当該接続されたウェブページのコンテンツに規定されたスパムキーワードがそのまま存している場合には当該電子メールをスパムメールとして推定し段階S24に進み前記発信元遮断リストDB（データベース）に該当電子メールの発信元を保存すると共に段階S26に進み前記URL遮断リストDB（データベース）に該当電子メールのダイナミックURLを保存し、段階S28に進み当該電子メールを「スパムメールボックス」に保存した後終了する。

【0030】

これにより、例えば下の〔表1〕及び〔表2〕は当該接続されたウェブページ（<http://www.ohmybuin.com/index.asp?ID=3956623>）のコンテンツソースのうち一部を抜粋して示したHTML文書であるところ、前記スパムキーワードとしては“やり友”、“オーガズム”、“成人ユーモア”、“変態”、“成人小説”、“オーラルセックス”、“性機具”または“自慰”などが含まれ得るし、このようなキーワードの内容がある電子メールがスパムメールとして容易に渡し出され得るであろう。

【0031】

従って、本発明のダイナミックURL接続を通じたスパムメール自動遮断方法によると、受信された電子メールにリンクされているURL情報を抽出して当該ウェブページに接続した後、予め規定された所定のスパムキーワードがある場合、これをスパムメールとして渡し出して自動で遮断することによって、スパムメールの遮断効率を増進させることがで

きる。

【0032】

【表1】

```
<a href="../communi/board.asp?code=1">やり友しまししょう</a></td>
<td width="26%">
<a href="../communi/board.asp?code=11">オーガズム体験談</a></td>
<td width="26%">
<a href="../communi/board.asp?code=21">写真交換しまししょう</a></td>
<td width="22%">
<a href="../communi/board.asp?code=31">成人ユーモア</a></td>
</tr>
<tr>
<td height="18">
<a href="../communi/board.asp?code=2">メル友しまししょう</a></td>
<td>
<a href="../communi/board.asp?code=12">変態体験談</a></td>
<td>
<a href="../communi/board.asp?code=22">動映像交換しまししょう</a></td>
<td>
<a href="../communi/board.asp?code=32">成人小説</a></td>
```

【0033】

【表2】

```
<a href="../communi/board.asp?code=3">友達になってあげますよ</a></td>
<td>
<a href="../communi/board.asp?code=13">オーラルセックス体験談</a></td>
<td>
<a href="../communi/board.asp?code=23">性機具交換しまししょう</a></td>
<td>
<a href="../communi/board.asp?code=33">体験手記</a></td>
</tr>
<tr>
<td height="18">
<a href="../communi/board.asp?code=4">私はイバン（女性）</a></td>
<td>
<a href="../communi/board.asp?code=14">白慰体験談</a></td>
<td>
```

【0034】

前述した本発明によるダイナミックURL接続を通じたスパムメール自動遮断方法に対す

範囲と発明の詳細な説明及び添付した図面の範囲内で色々と変形して実施することが可能であり、これまた本発明に属する。

【0035】

【発明の効果】

以上説明した通り、本発明のダイナミックURL接続を通じたスパムメール自動遮断方法によると、受信された電子メールのURL情報を抽出して該当ウェブサイトに接続した後、キーワード検索を通じて予め規定された所定のスパムキーワードがある場合、これをスパムメールとして分類して自動で遮断することによって、スパムメールの遮断効率をより増進させることができるだけでなく、既存システムで管理者が受信遮断リスト及び受信許可リストを探し出して登録する過程を経ずに自動で処理及び管理するので効率的かつ迅速であるという利点がある。

【図面の簡単な説明】

【図1】図1は一般的な電子メールシステムのネットワーク構成図である。

【図2】図2は本発明の一実施形態によるダイナミックURL接続を通じたスパムメール自動遮断方法を説明するためのフローチャートである。

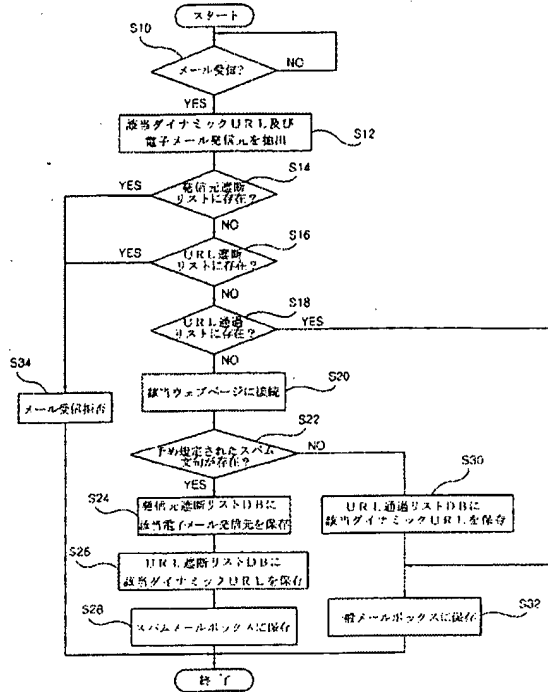
【図3】図3は本発明の一実施形態による受信された電子メールのポップアップウィンドウを示した図である。

【図4】図4は本発明の一実施形態による受信された電子メールのメッセージ原本を示した図である。

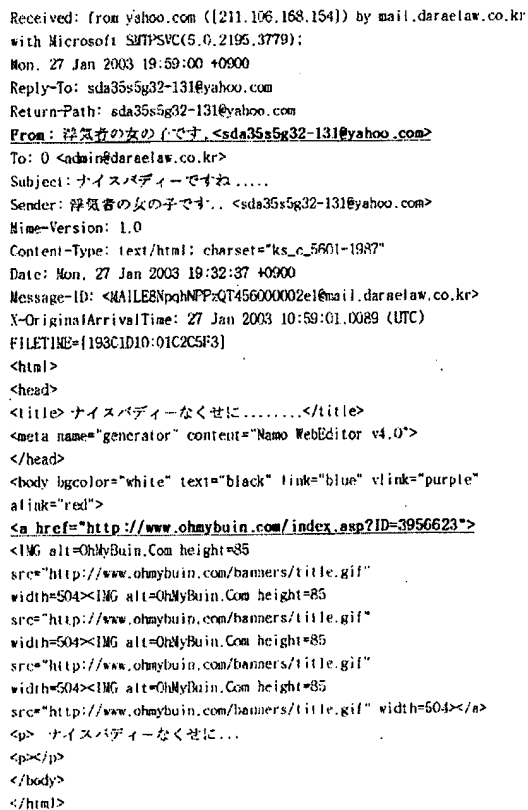
【符号の説明】

- 10：自体ウェブサイト
- 12：メールサーバ
- 14：ウェブサーバ
- 16：構内網
- 18：メールクライアント
- 20：外部ウェブサイト
- 22：ウェブサーバ
- 24：メールサーバ
- 30：インターネット
- 40：個人メールクライアント

【図2】



【図4】



- (72)発明者 ハ・ジュンホ
大韓民国442-739キュングド、スウォンシティ、パルダルク、ヨウントンドン、ファンゴル
ルージュコン・アパートメント107-203
- (72)発明者 アン・ジェコン
大韓民国461-824キュングド、スンナムシティ、スジョンク、テピョン1ドン7254-
1番、サムボージュテク、ガー302
- (72)発明者 カン・スホン
大韓民国690-802ジェジュド、ジェジュシティ、ノヒョンドン753番、エウテウムマ
ウル・アパートメント203-1106